REMARKS/ARGUMENTS

Claims 1-2 and 4-35 are pending in the application. Applicant amends claim 18, 21-22, and 25 and cancels claims 19 and 28. Applicant presents claims 1-2, 4-17, 20-27, and 29-35 for reconsideration, further examination, and allowance.

Discussion of Rejection Under 35 U.S.C. §112

Claim 21 was rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. In particular, the Examiner contends that Applicant's amendment of April 25, 2005 introduced new matter.

Although Applicant contends that no new matter was introduced into claim 21 with the prior amendment, Applicant amends claim 21 to remove the reference to a "non-secure" computer system. Applicant amends claim 21 to include "downloading communication link interface software to a processor from a HTTP server in a remote computer system." (*emphasis added to identify changes*). Support for the amendment can be found in Figure 1, where the HTTP server is identified as item 114. Additionally, support can be found throughout the specification, as filed. In particular, support can be found at page 8, ll. 16-23.

Applicant believes that the amendment overcomes the rejection under 35 U.S.C. §112 and respectfully requests withdrawal of the rejection to claim 21.

Discussion of Rejection Under 35 U.S.C. §103

Claims 1-2, 4-17, and 29-35 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over U.S. Patent No. 6,101,477 to Hohle et al. (hereinafter Hohle) in view of U.S. Patent No. 5,745,571 to Zuk (hereinafter Zuk). Claims 18-20 and 22-28 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over U.S. Patent No. 6,226,744 to Murphy et al. (hereinafter Murphy) in view of U.S. Patent No. 6,304,223 to Hilton et al. (hereinafter Hilton). Claim 21 was rejected under 35 U.S.C. §103(a) as allegedly unpatentable over Hohle in view of Murphy.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to

combine reference teachings. Second, there must be reasonable expectation of success. Finally, the prior art reference, or references when combined, must teach or suggest all of the claim limitations.

Applicant respectfully contends that the combination of references cited by the Examiner fails to teach or suggest all of the claimed limitations. Additionally, there is no motivation to combine the cited references in the manner suggested by the Examiner.

Claim 1 includes "demodulating an outgoing secure radio frequency signal transmitted from the smart card to produce an outgoing secure data signal." As discussed in the Response filed April 25, 2005, Hohle fails to describe a radio frequency signal transmitted from the smart card.

The Examiner alleges that Hohle describes a radio frequency communication channel with the smart card and cites Hohle Col. 3 ll. 31-51. However, this portion of Hohle describes contactless communication techniques that do not utilize a radio frequency communication channel. In the pertinent portion, Hohle states:

> That is, non-contact communication methods may be employed using such techniques as capacitive coupling, inductive coupling, and the like. As is known in the art, capacitive coupling involves incorporating capacitive plates into the card body such that data transfer with a card reader is provided through symmetric pairs of coupled surfaces, wherein capacitance values are typically 10-50 picofarads, and the working range is typically less than one millimeter. Inductive coupling employs coupling elements, or conductive loops, disposed in a weakly-coupled transformer configuration employing phase, frequency, or amplitude modulation. *Hohle* Col. 3 ll. 34-45.

Hohle describes capacitive plate coupling and inductive loop coupling, but does not describe the use of radio frequencies (RF) or a RF communication channel. Indeed, the coupling techniques described in the cited portion of Hohle are usually implemented exclusive of radio frequencies, and there is no indication that the capacitive or inductive coupling is used in conjunction with an RF communication channel.

Therefore, Applicant believes that claim 1 is allowable because Hohle fails to describe "demodulating an outgoing secure radio frequency signal transmitted from the smart

card." Hohle fails to describe the smart card transmitting a RF signal, nor a device that demodulates the RF signal.

Claims 17 and 29 include features similar to those discussed above in relation to claim 1. For example, claim 17 includes "demodulating an outgoing secure radio frequency signal at the smart card communication device to produce the outgoing secure data signal," and claim 29 includes "a radio frequency transceiver adapted to exchange secure data with a smart card through a radio frequency communication channel." Applicant believes that claims 17 and 29 are allowable at least for the same reasons as provided above in relation to claim 1.

With regard to claims 1-2, 4-17, and 29-35, the Examiner responds to Applicant's argument submitted in the Response filed April 25, 2005, and contends that the motivation to combine the teachings of Hohle and Zuk is provided in the references. The Examiner states that "adding the step of encryption as disclosed by Zuk would increase the security of the transmission and therefore discourage a third party from intercepting unencrypted data, as disclosed by Zuk."

Applicant respectfully contends that the generalized motivation alleged by the Examiner is rebutted by the specific language in Zuk. Zuk provides language that expressly teaches away from combining its teachings in a card system where the encryption technique is to be used repeatedly. Applicant notes that the prior art must be considered in its entirety, including disclosures that teach away from the claims. MPEP, §21241.02. A prima facie case of obviousness may be rebutted by showing that the art, in any material respect, teaches away from the claimed invention. *In re Geisler*, 116 F.3d 1465, 1471, 43 USPQ2d 1362, 1366 (Fed. Cir. 1997).

Zuk describes a public key encryption algorithm for initializing a smart card. *See Zuk*, Abstract and Col. 1 ll. 1-3. Zuk explicitly states:

> Public key techniques or algorithms, being computationally intensive have been considered too slow to execute and requiring too much memory in order to be practical for use on smart cards without additional specialised hardware. Most smart cards have very limited memory for both data and program storage, and employ microprocessors, such as 8 bit microprocessor, which are very slow compared with more powerful processors employed in personal computers and computer workstations. Many smart card applications require all of the program

> memory available on the card, and as much memory as possible for data, which *renders permanent hardware and software implementations of public key algorithms impractical. Zuk* Col. 2 ll. 15-27 (*emphasis added*).

Hohle, in contrast, "relates generally to the use of integrated circuit cards, or 'smartcards,' for commercial transactions, and more particularly, to methods and apparatus for conveniently storing, retrieving, and updating data related to a cardholder's travel information in the context of a distributed transaction system." *Hohle*, Col. 1, ll. 6-11. Therefore, Hohle is directed at methods and apparatus that are to be reused multiple times in processing cardholder travel information.

The environment where the smartcard methods and apparatus are continually reused is precisely the environment that Zuk states its invention is unsuitable. Zuk provides explicit teaching away from the combination in contrast to the generalized motivation to combine offered by the Examiner. Thus, Applicant believes that claims 1-2, 4-17, and 29-35 are allowable for the independent reason that there is no motivation to combine the teachings of Hohle with Zuk.

Claims 2, 4-16, and 30-35 depend from one of claims 1, 17, and 29 and are believed to be allowable at least for the reason that they depend from an allowable base claim. Applicant respectfully requests reconsideration and allowance of claims 2, 4-16, and 30-35.

Applicant respectfully requests reconsideration and allowance of claims 1-2, 4-17, and 29-35 because Hohle and Zuk fail to describe the smart card transmitting a RF signal. Additionally, there is no motivation to combine the teachings of Hohle with Zuk, because Zuk expressly teaches away from such combination. The Examiner has provided no reasons as to why the express statements provided in Zuk would be ignored by one of ordinary skill in the art.

Claim 21 includes the feature of "exchanging secure data between the smart card and a smart card communication device through a radio frequency communication channel." As described above, Hohle fails to describe a radio frequency communication channel. The Examiner concedes that Murphy does not describe a radio frequency communication channel with the smart card. Therefore, the combination of references fails to teach or suggest all claimed limitations. Applicant respectfully requests reconsideration and allowance of claim 21.

Claim 18 includes "performing a security function at the smart card on secure data received from the central computer system." This feature is not taught nor suggested by either Murphy or Hilton. Murphy teaches a smart card used to authenticate a user to a secure system. The smart card does not perform a security function on any data received from the central computer system. Because the smart card is used to authenticate a user with the secure system, typically no data is transmitted to the smart card, and there is no indication that the smart card performs a security function on any received data.

Hilton also fails to describe the smart card performing a security function on received data. Hilton describes a smart card reader in which the user inserts the smart card at least partially into a cavity of the device. *Hilton*, Abstract. Hilton does not describe the smart card functions or security functions that can be performed by the smart card.

Applicant respectfully requests reconsideration and allowance of claim 18, because the cited references fail to teach or suggest all claim limitations. Claims 22 and 25 include similar features of the smart card performing a security function on received data. Applicant respectfully requests reconsideration and allowance of claims 22 and 25 at least for the same reasons provided above in relation to claim 18.

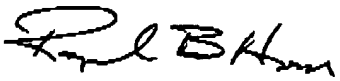
Claims 20, 23-24, and 26-27 depend from one of claims 18, 22, or 25 and are believed to be allowable at least for the reason that they depend from an allowable base claim. Applicant respectfully requests reconsideration and allowance of claims 20, 23-24, and 26-27.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 858-350-6100.

Respectfully submitted,



Raymond B. Hom
Reg. No. 44,773

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 858-350-6100
Fax: 415-576-0300

RBH:jo
60568769 v1